

9/PRTS

明細書

10/537279  
JC17 Rec'd PCT/PTO 27 MAY 2005

インターネット接続システム及びクライアント機器への接続をルーティン  
グするためのサーバ

5

#### 関連する出願への参照

この出願は、日本国特許出願、特願2002-348543号、特願20  
03-161246号、特願2003-345390号に基づくパリ条約第  
4条（及びこれに対応する各国の規定）の優先権を主張し、これら特許出願  
10 の明細書及び図面に記載された事項はこの参照により本出願の明細書に全体  
的に記載されたものとする。

#### 技術分野

この発明は、IPv4（Internet Protocol version 4）が普及した現状  
15 のインフラ環境の下で、次世代のIPであるIPv6（Internet Protocol  
version 6）によるネットワークの構築を実現し、家庭内のIPv6環境に  
サーバからサービスを提供するためのシステム及びこれに使用される前記サ  
ーバに関するものである。

#### 20 背景技術

一般に、インターネットを中心とした公衆ネットワークを通じたサービス  
提供環境においては、全ての情報の価値は、クライアント側ではなく、サー  
バ側に集まるようになっている。

すなわち、各クライアントである端末機器は、基本的にインターネット上  
25 の情報を閲覧するための単なるビューワーにしか過ぎない。また、各クライ  
アントはインターネット側に様々な情報の要求を発しており、インターネッ  
ト側ではそのような各クライアントの情報を得ることができる。すなわち、  
全ての情報は、インターネット側に集められ、インターネット側からは定型

的な情報が一方的に与えられるに過ぎない。このため、クライアント端末機を製造しているメーカーは付加価値が生み出しづらい状況となっている。

このような状況を変えるためには、アクセス方向を逆行させ、サーバとクライアントの立場を逆転させることが必要である。すなわち、インターネット  
5 トに接続される家庭内ネットワークがある場合、インターネット側から家庭内ネットワークへのアクセスが開始され、家庭内ネットワーク側からインターネット側へサービスが提供されるような状態を作り出す必要がある。

このためには、ホームネットワークに接続された機器のそれぞれが、インターネット側からユニークに特定できること、家庭内のルーティング  
10 の問題、セキュリティの問題を解決する必要がある。このような課題に対応し、ひとつの解決を見出せる技術として、I P v 6 (Internet Protocol version 6: 第6世代インターネットプロトコル) がある。

しかしながら、現在の日本のキャリアやインターネットサービスプロバイダを取り巻く環境を鑑みると、I P v 6の普及にはかなりの時間がかかるものと  
15 のと考えられる。例えば、現在使用しているI P v 4の機材償却に最低2年～3年は必要であり、テスト的なサービスが行われているのみである。

今すぐにメーカーがI P v 6対応ネットワークを実現するには、I S Pレベルのサービスにまで手を出すしかないが、非常にコストがかかることであり、多くのメーカーにとって現実的ではない。

20 家庭内ネットワークの事情が様々で非常に大きく異なることや、キャリアやI S Pによって接続の仕組みが大きく異なることもあり、これらの差を吸収して画一的なアプローチでI P v 6環境を実現するための仕組みが必要である。

この発明はこのような事情に鑑みてなされたもので、比較的簡易な手段により  
25 よりI P v 6の恩恵を受けることができ、かつ、クライアント側の機器を製造するメーカーが独自の付加価値を見出すことができるインターネット接続システムを提供することを目的とするものである。

## 発明の開示

上記目的を達成するため、この発明の第1の主要な観点によれば、クライアント機器が接続され第1の通信プロトコルで通信が行われる第1のネットワークに設けられた中継装置と、この中継装置が第2のネットワークを通し

5 第2の通信プロトコルで接続されるサーバとを有し、前記中継装置には、前記クライアント機器の前記第1の通信プロトコルでのグローバルアドレスを記憶する前記クライアント機器グローバルアドレス記憶部と、前記サーバの第2のプロトコルでのグローバルアドレスを記憶するサーバアドレス記憶部と、この記憶部に記憶されたサーバのグローバルアドレスに基づき前記クライアント機器からの接続を前記サーバを経由するようにルーティングするた

10 めの第1のルーティング装置と、第1のプロトコルでのパケットを第2のプロトコルでカプセリング／デカプセリングすることで前記サーバとの間で第1のプロトコルのトンネリング接続を確立する第1のパケット処理装置と、が設けられており、前記サーバには、前記中継装置との間のトンネリング

15 接続を可能にするために第1のプロトコルでのパケットを第2のプロトコルでカプセリング／デカプセリングする第2のパケット処理装置と、前記中継装置に接続された前記クライアント機器の第1のプロトコルでのグローバルアドレスを前記中継装置の第2のプロトコルでのグローバルアドレスに関連付けて管理する端末機器グローバルアドレス管理装置と、この管理装置で

20 管理された前記端末機器のグローバルアドレスに基づいて前記中継装置へのルーティングを行う第2のルーティング装置と、が設けられていることを特徴とするインターネット接続システムが提供される。

このような構成によれば、家庭内のネットワークとインターネット側サーバとの間で、IPv6パケットがトンネリング接続により送受信される。そして、家庭内ネットワークに存在する端末機器を前記サーバを通して外部からユニークに認識することができ、制御できる。そして、全ての通信はキャリアやISPに関らず、前記インターネット側サーバを通して行われることになるから、前記家庭内の端末機器及びその端末機器への接続の全てを前記

インターネット側サーバの所有者若しくは製造者が自由に設定・制御することが可能になる。

すなわち、従来問題であった、IPv6とIPv4が混在する中でのIPv6機器の個体認識、家庭内ルーティング及びセキュリティの問題を全て解決でき、極めてオープンかつ、クローズドなネットワークの構築を実現することが可能になる。

ここで、前記第1のプロトコルと第2のプロトコルは、異なるプロトコルであっても良いし、同じプロトコルであっても良いが、最も好ましい実施形態においては、前記第1のプロトコルはIPv6であり、第2のプロトコルはIPv4である。

この発明の1の実施形態によれば、前記サーバには、前記クライアント機器若しくは／及び前記中継装置が所定の機種であるかを判別する機種判別部が設けられている。この場合、前記サーバには、前記機種判別部により前記クライアント機器若しくは中継装置が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部が設けられていることが好ましい。また、前記サーバには、前記機種判別部による判断結果に基づいて前記クライアント機器に送信する命令をこのクライアント機器を制御するための所定形式のコマンドに変換するコマンド変換部が設けられていても良い。さらに、前記サーバには、前記機種判別部による判断結果に基づいて前記クライアント機器を制御するクライアント機器制御部が設けられていることが望ましい。

他の1の実施形態によれば、前記サーバには、前記クライアント機器若しくは／及び中継装置が接続された第1のネットワークの環境が所定の種別であるかを判別するネットワーク種別判別部が設けられている。この場合、前記サーバは、前記クライアント機器若しくは中継装置が接続されたプライベートネットワーク環境が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部を有することが好ましい。さらに、この場合、前記サーバは、

前記クライアント機器若しくは／及び中継装置の動作状態、使用状態、位置情報の少なくとも1つ又は複数の情報を取得する状態情報取得部を有することが望ましく、この状態情報取得部は、前記クライアント機器の機種に応じた方法で前記クライアント機器の動作状態、使用状態、位置情報の少なくとも1  
5 5 1 つ又は複数の情報を取得するものであることがさらに好ましい。

さらなる他の1の実施形態によれば、前記サーバは、前記クライアント機器若しくは中継装置のアドレス、動作状態、使用状態、位置情報の少なくとも1つ又は複数の情報を組み合わせた情報に基づいて前記クライアント機器若しくは中継装置を検索する検索部を有する。この場合、この検索部は、前  
10 記中継装置毎にこの中継装置に接続されたクライアント機器を一覧表示する手段を有することが好ましい。そしてさらにこの場合、前記サーバには、前記クライアント機器を制御するクライアント機器制御部が設けられており、このクライアント機器制御部は、前記一覧表示から特定のクライアント機器を選択することでこのクライアント機器に対応するクライアント制御プログラムを起動させるものであることが望ましい。  
15 15 1 ラムを起動させるものであることが望ましい。

更なる他の1の実施形態によれば、前記サーバには、前記クライアント機器への接続要求に基づいて前記クライアント機器の第1の Protokol でのグローバルアドレスの検索を行うクライアント機器アドレス検索部が設けられている。この場合、前記サーバには、前記クライアント機器への接続要求を行  
20 20 1 った者の認証を行って前記クライアント機器への接続を許可若しくは否認する接続要求者認証部が設けられていることが好ましい。

更なる他の1の実施形態によれば、このシステムはさらに、前記中継装置とサーバとの間のトンネリング接続情報を管理するトンネリング接続情報管理装置を有し、このトンネリング接続情報管理装置は、前記サーバの第2の  
25 25 1 Protokol でのグローバルアドレスを前記中継装置に通知し、前記中継装置の第2の Protokol でのグローバルアドレス及び前記クライアント機器の第1の Protokol でのグローバルアドレス若しくはその一部を前記サーバに通知する。この場合、前記トンネリング接続情報管理装置は、前記中継装置若

しくはサーバの認証を行い、その結果が肯定的である場合に前記通知を行うことが好ましい。

更なる別の 1 の実施形態によれば、前記サーバは、前記クライアント機器への／からの通信を所定のルールでフィルタリングするフィルタリング処理装置を有する。この場合、前記サーバは、前記所定のルールを編集するためのインタフェースを提供するフィルタリングルール設定部をさらに有することが好ましい。

更なる別の 1 の実施形態によれば、前記中継装置には、前記クライアント機器が所定の機種であるかを判別する機種判別部が設けられている。この場合、前記中継装置には、前記機種判別部により前記クライアント機器が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断する通信セッション切断部が設けられていることが好ましい。

この発明の第 2 の主要な観点によれば、クライアント機器が接続され第 1 の通信プロトコルで通信が行われる第 1 のネットワークに設けられた中継装置と、この中継装置が第 2 のネットワークを通し第 2 の通信プロトコルで接続されるサーバと、を有するインターネット接続システムに使用される前記中継装置であって、前記中継装置には、前記クライアント機器の前記第 1 の通信プロトコルでのグローバルアドレスを記憶する前記クライアント機器グローバルアドレス記憶部と、前記サーバの第 2 のプロトコルでのグローバルアドレスを記憶するサーバアドレス記憶部と、この記憶部に記憶されたサーバのグローバルアドレスに基づき前記クライアント機器からの接続を前記サーバを経由するようにルーティングするための第 1 のルーティング装置と、第 1 のプロトコルでのパケットを第 2 のプロトコルでカプセル化／デカプセル化することで前記サーバとの間で第 1 のプロトコルのトンネリング接続を確立する第 1 のパケット処理装置と、が設けられていることを特徴とする中継装置が提供される。

この発明の第 3 の主要な観点によれば、クライアント機器が接続され第 1 の通信プロトコルで通信が行われる第 1 のネットワークに設けられた中継装

- 置と、この中継装置が第2のネットワークを通し第2の通信プロトコルで接続されるサーバと、を有するインターネット接続システムに使用される前記サーバであって、前記サーバには、前記中継装置との間のトンネリング接続を可能にするために第1のプロトコルでのパケットを第2のプロトコルでカプセリング／ディカプセリングする第2のパケット処理装置と、前記中継装置に接続された前記クライアント機器の第1のプロトコルでのグローバルアドレスを前記中継装置の第2のプロトコルでのグローバルアドレスに関連付けて管理する端末機器グローバルアドレス管理装置と、この管理装置で管理された前記端末機器のグローバルアドレスに基づいて前記中継装置へのルーティングを行う第2のルーティング装置と、が設けられていることを特徴とするサーバが提供される。

- この発明の第4の主要な観点によれば、第1のネットワークに設けられた中継装置と、この第1のネットワークに接続されたクライアント機器が前記中継装置及びインターネットを通して接続されるサーバと、を有するインターネット接続システムに使用される前記サーバであって、前記中継装置に接続された前記クライアント機器のアドレスを前記中継装置のアドレスに関連付けて管理するクライアント機器アドレス管理装置と、前記インターネットから前記クライアント機器宛の接続を、前記管理装置で管理された前記クライアント機器のアドレスに基づいて前記クライアント機器が接続された中継装置へルーティングするルーティング装置と、前記クライアント機器若しくは／及び前記中継装置が所定の機種であるかを判別する機種判別部と、前記機種判別部による判断結果に基づいて前記クライアント機器に送信する命令をこのクライアント機器を制御するための所定形式のコマンドに変換するコマンド変換部とを有することを特徴とするサーバが提供される。

- このような構成によれば、家庭内ネットワークに存在する端末機器の機種を前記サーバを通して外部からユニークに認識することができる。そして、その機種に応じて前記端末機器を制御することができる。そして、全ての通信はキャリアやISPに関らず、前記インターネット側サーバを通して行わ

れることになるから、前記家庭内の端末機器及びその端末機器への接続の全てを前記インターネット側サーバの所有者若しくは製造者が自由に設定・制御することが可能になる。

この発明の 1 の実施形態によれば、さらに、前記機種判別部により前記クライアント機器若しくは中継装置が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部が設けられている。

また、この発明の別の 1 の実施形態によれば、前記クライアント機器は、前記中継装置とは通信可能であるが、自らはインターネットに接続することができない周辺装置を含むものである。

さらなる別の 1 の実施形態によれば、さらに、前記クライアント機器若しくは／及び中継装置が接続された第 1 のネットワークの環境が所定の種別であるかを判別するネットワーク種別判別部が設けられている。この場合、さらに、前記クライアント機器若しくは中継装置が接続されたプライベートネットワーク環境が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部を有することが好ましい。

さらなる別の 1 の実施形態によれば、さらに、前記クライアント機器若しくは／及び中継装置の動作状態、使用状態、位置情報の少なくとも 1 つ又は複数の情報を取得する状態情報取得部を有するものである。この場合、前記状態情報取得部は、前記クライアント機器の機種に応じた方法で前記クライアント機器の動作状態、使用状態、位置情報の少なくとも 1 つ又は複数の情報を取得するものであることが好ましい。また、前記クライアント機器を制御するクライアント機器制御部が設けられており、このクライアント機器制御部は、前記クライアントの動作状態、使用状態、位置情報の少なくとも 1 つの情報をユーザに表示する手段を有するものであることがさらに望ましい。

また、前記クライアント機器若しくは中継装置のアドレス、動作状態、使用状態、位置情報の少なくとも 1 つ又は複数の情報を組み合わせた情報に基



づいて前記クライアント機器若しくは中継装置を検索する検索部を有する。  
この検索部は、検索されたクライアント機器をその動作状態と共に一覧表示  
する一覧表示手段を有することが好ましい。また、前記一覧表示手段は、前  
記中継装置毎にこの中継装置に接続されたクライアント機器を一覧表示する  
5 ものである。さらに、前記クライアント機器を制御するクライアント機器制  
御部が設けられており、このクライアント機器制御部は、前記一覧表示から  
特定のクライアント機器を選択することでこのクライアント機器に対応する  
クライアント制御プログラムを起動させるものであることが好ましい。

更なる別の1の実施形態によれば、前記中継装置は、前記クライアント機  
10 器に設けられているものである。

別の1の実施形態によれば、さらに、前記中継装置との間のトンネリング  
接続を可能にするために第1のプロトコルでのパケットを第2のプロトコル  
でカプセリング／ディカプセリングする第2のパケット処理装置と、前記中  
継装置に接続された前記クライアント機器の第1のプロトコルでのグローバ  
15 ルアドレスを前記中継装置の第2のプロトコルでのグローバルアドレスに関  
連付けて管理する端末機器グローバルアドレス管理装置と、この管理装置で  
管理された前記端末機器のグローバルアドレスに基づいて前記中継装置への  
ルーティングを行う第2のルーティング装置と、が設けられている。前記第  
1のプロトコルと第2のプロトコルは、異なるプロトコルであっても良いし  
20 、同じプロトコルであっても良い。

また、さらに、前記クライアント機器への接続要求に基づいて前記クライ  
アント機器の第1のプロトコルでのグローバルアドレスの検索を行うクライ  
アント機器アドレス検索部が設けられていることが好ましい。この場合、さ  
らに、前記クライアント機器への接続要求を行った者の認証を行って前記ク  
25 ライアント機器への接続を許可若しくは否認する接続要求者認証部が設けら  
れていることが好ましい。

また、このサーバはさらに、前記中継装置とサーバとの間のトンネリング  
接続情報を管理するトンネリング接続情報管理装置を有し、このトンネリン

- グ接続情報管理装置は、前記サーバの第2の Protokolでのグローバルアドレスを前記中継装置に通知し、前記中継装置の第2の Protokolでのグローバルアドレス及び前記クライアント機器の第1の Protokolでのグローバルアドレス若しくはその一部を取得するものである。ここで、前記トンネリング
- 5 グ接続情報管理装置は、前記中継装置の認証を行い、その結果が肯定的である場合に前記通知を行うことが好ましい。

- 更なる別の1の実施形態によれば、さらに、前記クライアント機器への／からの通信を所定のルールでフィルタリングするフィルタリング処理装置を有する。この場合、さらに、前記所定のルールを編集するためのインタフェースを提供するフィルタリングルール設定部を有することが好ましい。
- 10

この発明のインターネット接続システムに使用されるサーバによれば、比較的簡易な手段によりIPv6の恩恵を受けることができ、かつ、クライアント側の機器を製造するメーカーが独自の付加価値を見出すことができるインターネット接続方法を提供することができる。

- 15 この発明の更なる他の特徴と顕著な効果は次の発明を実施するための最良の形態の項に記載された実施形態及び図面を参照することによって当業者にとって理解される。

#### 図面の簡単な説明

- 20 図1は、この発明の一実施形態に係るネットワーク構成の例を示す図。  
図2は、同じくInterBOXの例を示す概略構成図。  
図3は、同じくInterServerの例を示す概略構成図。  
図4は、フィルタ部の概略構成を示す図。  
図5は、フィルタ部での処理を示すフローチャート
- 25 図6は、IPv6端末検索部の概略構成を示す図。  
図7は、検索画面の例を示す図。  
図8は、InterBOXに関する検索結果リスト表示の例を示す図。  
図9は、IPv6端末制御部による制御の概念を示す図。

図10は、この実施形態における通信例を示す機能図。

図11は、この実施形態における別の通信例を示す機能図。

図12は、InterBOX若しくはIPv6端末のセットアップ例を示す図。

- 5 図13は、InterBOXとInterServer間のトンネリング接続の例を示す図。

#### 発明を実施するための最良の形態

以下、この発明の実施の形態を図面を参照して説明する。

- 10 図1は、この実施形態に係るネットワーク構成の例を示したものである。
- 図中1は、IPv6（第1の通信プロトコル）で通信を行う各種クライアントIPv6端末機器2（以下「IPv6端末」という）…が接続されてなるIPv6ホームネットワークである。このホームネットワーク1は例えば各家庭に導入されたLANによって構成される。
- 15 そして、このホームネットワーク1は、InterBOX3（この発明の「中継装置」）及び通信キャリア/ISPを介してインターネット網4に接続されている。このインターネット網4では、前記IPv6とは異なり現在広く普及しているIPv4（第2の通信プロトコル）を用いて通信が行なわれるようになっている。
- 20 そして、このインターネット網4には、前記ホームネットワーク1上のIPv6端末2の通信を制御するInterServer6（この発明の「サーバ」）が接続されている。このInterServer6は、後で詳しく説明するように、前記IPv6端末2と、インターネット網4上若しくは他のホーム/グローバルネットワーク1a、1b上の全てのIPv6端末2a、2b、IPv6サーバ7との間の接続を仲介する機能を有するものである。
- 25

ここで、InterBOX3とInterServer6は、同じメーカー若しくは統一された規格の下に製造されることが意図されており、予め連

- 動するように設計されたものである。そして、InterBOX3には、予めInterServer6のIPv4でのグローバルアドレスが記憶されていて、ISPやキャリアを問わず常に前記InterServer6にルーティングされて接続されるようになっている。また、前記ホームネットワーク1に接続されるIPv6端末2についても、前記InterBOX3等と同じメーカー若しくは統一された規格の下に製造されたものであることが意図されており、このIPv6端末2に割当てられたIPv6でのグローバルアドレス、その他の情報に基づいて、前記InterServer6側でその端末の種別（機種）等を特定できるようになっている。
- 10      ここで、IPv6端末2のIPv6アドレスの割振りについては種々の手法が考えられる。IPv6アドレスは128ビットで構成され、その前半部に設定されNICやISPから割り振られる「プレフィックス」部と、後半部分に設定されユーザが独自に生成する「インタフェースID」部とからなる。この例でも、各メーカーに割り振られたプレフィックスと、各端末固有のMACアドレスを用いて生成するインタフェースIDとを組み合わせる用
- 15      いる。このIPv6アドレスは、端末2の出荷前にすでに決定されているものであっても良いし、InterBOX3に接続することでこのInterBOX3のIPv6アドレスプレフィックスと自己のMACアドレスを用いて自動的に生成されるものであっても良い。また、前記IPv6端末2が自
- 20      らはインターネットに接続できないビデオやテレビのような家電であっても良い。この場合には、この家電が通信できるインタフェース（IEEE1394）を前記InterBOXに備えておき、各家電のID（ユニークID）に対して仮想IPアドレスを割り付けておけば良い。

図2は、前記InterBOX3を示す概略構成図である。

- 25      このInterBOX3は、前記InterServer6のIPv4でのグローバルアドレスを記憶するサーバアドレス記憶部10と、このInterServer6のアドレスに基づいてInterServer6との間でトンネリング接続を確立するトンネリングセッション確立部11と、IP

v6でのパケットをIPv4でカプセリング／ディカプセリングして前記InterServer6との間でトンネリング送受信を行うためのカプセリング処理部12と、前記ディカプセリングされた前記InterServer6側からのパケットを所望のIPv6端末2にルーティングするためのルーティング処理部13と、パケットの送受信を行うパケット送受信部14とを有する。又、このInterBOX3は、IPv6端末2のアドレスをInterBOX3に割当てられるプレフィックスを用いて生成する場合等のためにプレフィックス記憶部15（アドレス生成部）が設けられている。

このような構成によれば、前記IPv6端末2からのパケット若しくはIPv6端末2へのパケットを前記InterServer6とInterBOX3との間に確立されたIPv4によるトンネルを通して送受信することができる。

また、図3は、前記InterServer6を示す概略構成図である。

このInterServer6には、InterBOX3のIPv4でのグローバルアドレス16a及び前記クライアント機器のIPv6でのグローバルアドレス16bを関連付けて記憶するアドレス記憶部16と、前記InterBOX3のアドレスに基づいてこのInterBOX3との間でトンネリング接続を確立するトンネリングセッション確立部17と、前記IPv6端末2との間の通信を可能にするためにIPv6でのパケットをIPv4でカプセリング／ディカプセリングするカプセリング処理部18と、前記IPv6端末2と他の端末・サーバとの間の通信をルーティングするルーティング部19とを有する。また、このInterServer6は、前記IPv6端末2のIPv6アドレスに基づいてこのIPv6端末2の種別を判別する機種判別部21と、この判別結果に基づいて前記IPv6端末2への命令を所定のコマンドに変換して設定するコマンド設定部22と、トンネル送信されるIPv6パケットを所定のルールでフィルタリングするフィルタ部23と、所定の場合通信セッションを切断する通信セッション切断部24とを有する。そして、パケットの送受信は送受信処理部25によって行われる

ようになっている。

また、このInterServer6は、ユーザ管理サーバ30に接続されている。このユーザ管理サーバ30は、後で詳しく説明するように、各InterBOX3や各IPv6端末2のユーザの情報を管理するものであり、各ユーザのID、パスワード及び課金情報等の会員情報の他、IPv6ブ  
5 レフィックスや機種情報等を格納するユーザ情報管理DB31を有する。

さらに、このInterServer6は、インターネット4（IPv4ネットワーク）上で公開されたWebサーバ32を有し、前記InterBox3やIPv6端末2のユーザからの要求を受け付けて各種設定を行わせることを可能にする。例えば、前記フィルタ部23によるフィルタルールの  
10 少なくとも一部は、このWebサーバ32を通し、前記ユーザによって適宜変更可能である。なお、このWebサーバ32へのアクセスはInterBOX3及びInterServer6経由であっても良いし、これらを経由しないインターネット4経由であっても良い。

前記フィルタ部23は、図4に示すように、フィルタルール記憶部33と、  
15 フィルタルール設定部34とを有する。このフィルタルール記憶部33及びフィルタルール設定部34は、インターネット上に公開された前記Webサーバ32に接続されており、前記Webサーバ32には図3に示すようにInterServer対話用インタフェース生成部35がインストール  
20 されている。このWebサーバ32に接続したユーザは、このインタフェース生成部35によって生成されたインタフェースを自己の端末上に表示することで、フィルタルールの入力・変更ができるようになっている。ここで設定できるフィルタルールとしては、例えば、セキュリティに関するものが考えられる。

25 セキュリティ上のフィルタルールとしては、大きく分けて、①外部からのホームネットワーク側へのアクセスを一切認めない、②外部からのホームネットワーク側へのアクセスを、事前に認めたサーバ（Webサイト）やネットワークから以外認めない、③外部からのホームネットワーク側へのアクセ

スを一切制限しない、が考えられる。また、この場合のフィルタリング方法としては、一切アクセスを認めない方法であっても良いが、特定のポートのみ通すようにしても良い。

- ここで、ホームネットワーク 1 から外部へのアクセスについても、事前に
- 5 設定したサーバにはアクセスできないよう制限できるようにすると、子供が有害なコンテンツにアクセスするのを防げたり、ユーザが一般に不正(トラップを仕掛けているような)なサイトにアクセスすることを防ぐことが可能になる。

- なお、このフィルタルールの設定は、前記Webサーバ 3 2 に設けられ前
- 10 記ユーザ管理サーバ 3 0 に接続可能なユーザ認証部 3 6 によるID及びパスワードの認証後に行えるようになっている。

- 前記フィルタルール設定部 3 4 は、上述したようにユーザの入力に基づいてフィルタルールを設定するが、これ以外に、ユーザからの設定によらずに前記ユーザ管理サーバ 3 0 に格納された会員情報(課金情報や端末機種の情報)
- 15 報)に基づいて自動的にフィルタルールを生成する機能を有する。例えば、前記会員の属性や会費納付状況に応じて、接続を許可しなかったり、特定のサーバにのみ接続可能にするなどのゲートウェイとしての設定が行える。

- このゲートウェイとしてのフィルタルールは、このInterServer 6 を通して有料ビジネスを提供するベンダーをコントロールするために使用
- 20 できる。例えば、図3に示すように、前記InterServer 6 に代理サーバ 3 8 を設けてユーザのアクセス先をDB 3 9 に管理しておき、ユーザが前記フィルタルール設定部 3 4 に設定されたアクセス先にしか接続できないようにしてもよい。この場合、前記ユーザID及びパスワードに加えてそのユーザがどのサービス(サーバ)をどのような条件で契約しているかを
- 25 前記ユーザ管理DB 3 1 で管理しておき、その条件に応じて、トランザクションをコントロールする機能を実装するようにすることが好ましい。また、特定のベンダーに関しては、登録手続きが完了していないユーザに対してはサンプルだけを見せて本体は見せないようにする等の設定をしてもよい。

図5は、このフィルタ部23での処理を示すフローチャートである。まずトンネリングセッションが開始されると、前記ユーザ管理サーバ30から受け取った会員情報に基づいてフィルタルールを設定する（ステップS1）。  
5 ついで、前記代理サーバ38から前記ユーザの接続要求先の情報（例えばWebサイトのアドレス）を受け取る（ステップS2）。ついで、この接続先の情報を前記フィルタルールに適用し、接続の可否を判断し（ステップS3）、接続を許可できない場合には前記通信セッション切断部24で通信セッションを切断する（ステップS4）。接続許可できる場合には、セッションが未だ有効であるかを判断し（ステップS5）、有効である場合には前記ステップS2～S5の処理を繰り返す。有効でない場合には処理を終了する。  
10

また、前記代理サーバ38で、データの通信量を計測しておき、課金を払っていない者からのアクセスは認めないようにしても良い。この場合、ベンダーには、ユーザのIDのみを教え、そのユーザのパスワードやIPアドレスは案内しないようにする。これにより、ユーザはInterServer6  
15 用の一対のID及びパスワードを管理していればよいことになる。また、IPアドレスはユーザの都合その他の理由で変更する場合もあるので、つどにIDをキーに確認してもらうのがシステムの整合性の点でも適当であり、ベンダー側でデータをもって不当にアクセスする危険も排除できるために適当である。  
20

前記フィルタルールの執行及びそれに基づいた通信セッションの切断や接続等の実行は、前記通信セッション切断部24によって行なわれる。なお、設定されたフィルタルールを用いたフィルタ方法、ゲートウェイ方法、その他の方法は公知であるのでその説明は省略する。

25 また、前記InterServer6は、前記IPv6端末2のアドレスを知らない者がこのIPv6端末2の検索を行うための機能を提供するIPv6端末検索部26（図3）を有する。この検索部26は、ユーザが指定した情報、例えばIPv6端末2の稼動状態やネットワークの稼動状態等に基づ



づいて所望のIPv6端末2を検索し特定する。

このため、この検索部26は、図6に示すように前記IPv6ネットワーク及びInterBOX3に接続されたIPv6端末2の稼動状態やネットワークの状態等の状態情報を受け取る状態情報受取部40と、この情報を前  
5 記IPv6端末のIPアドレスやInterBOX3のIPアドレスに関連付けて蓄積する状態情報蓄積部41と、IPv6端末制御部42とを有する。

前記状態情報受取部40は、前記IPv6端末2を収容するプレフィックス若しくはドメイン（IPv6ネットワーク若しくはInterBOX3）  
10 ごとに各IPv6端末2の状態を受け取る。この情報受取部40は、前記プレフィックス及びドメイン毎に所定の周期で状態を問い合わせることによってその状態を受け取るものであっても良いし、各プレフィックス若しくはドメインに対する参照の要求があった時点で問い合わせる状態を取得するものであっても良い。前者の方法の場合、例えば、前記InterBOXアドレス  
15 ス格納部16aに登録されたInterBOX毎に1分毎に各端末2の電源のON/OFFの問い合わせを行う。

前記状態情報蓄積部41は、上記各IPv6端末2の状態情報を、このIPv6端末及びInterBOX3に関連付けて格納する。ここで、取得する状態情報は、大きく分けて、動作状態、使用状態、位置情報、特性を表す  
20 情報、ノード（InterBOX3やIPv6端末2）が保有する情報を示す情報、その他ノードを特定するのに有効な情報の少なくとも1つ又は複数である。

動作情報としては、少なくとも電源の状態、ネットワーク接続状態、通信状態の1つあるいは複数である。使用状態としては少なくとも利用者に関する  
25 情報、動作時間に関する情報、負荷に関する情報の1つ又は複数である。位置情報は、少なくとも地理的な位置や座標情報、郵便番号、部屋番号等である。特性を示す情報としては、ノードの種類、機能、形状、色彩、装置情報、ソフトウェア情報、機能、管理者等の情報のうちの1つ又は複数である。

。

また、前記IPv6機種判別部21で判別された機種も個々に状態情報として格納する。前記状態情報受取部40は、この機種情報に基づいて前記IPv6端末2から得られる情報を特定し、必要な情報をそれらに適合した形式で取得することができるようになっている。

前記検索部26は、また、前記ユーザ管理サーバ30に接続して前記検索若しくは接続要求を行う者を認証し、検索及び接続要求を許可する接続要求認証部27を備えている。例えば、ユーザのホームネットワーク（InterBOX3）に対してはそのネットワークに関して接続を許可された特定のユーザ以外の検索及び接続は許可されない。この認証部27で肯定的であると判断された場合には、この検索部26は前記状態情報蓄積部41及びアドレス記憶部16にアクセスして所望の端末2のアドレスを検索（InterBOX3を特定）する。

検索の結果は、例えば、ユーザがパーソナルコンピュータを使用して外部から自己のホームネットワークのInterBOX3を検索した場合には、そのInterBOX3に接続された全てのIPv6端末機2がその状態と共にリスト表示されるようになっていても良い。図7は、検索画面の例、図8は、検索の結果特定されたInterBOXに関するリスト表示の例を示したものである。図7に示した検索用インタフェースの例では、InterBOX3を検索するための入力欄43と、IPv6端末2を検索するための入力欄44が設けられており、どちらからでも検索を行えるようプログラムされている。

また、図8の検索結果リスト表示の例では、前記InterBOX3に接続された全ての端末2が、所有者、状態、種別及び機種名の情報と共にリスト表示されている。そして、図に45で示す操作画面表示ボタンを押すことで、前記端末制御部42が起動され当該端末2の種別及び機種に応じた操作画面（図示しない）が表示される。

図9は、前記制御部42による制御の概念図を示したものである。

まず、IPv6端末2は、InterBOX3がトンネリングセッションを通してInterServer6に接続している状態で、前記状態情報取得部40からの要求によりその稼動状態を通知する（ステップS11）。このとき、IPv6端末2側から前記制御部42にログインしなければ上記の  
5 ような稼動状態の取得が行えないようにしておいても良い。前記稼動状態の取得は、一定周期で行われ前記状態情報蓄積部41に蓄積されかつ更新される（ステップS12）。

ついで、前記IPv6端末2のユーザが外部からID及びパスワードを用いて外部からログインし、前記リストから上述したように制御したい端末を  
10 特定して前記制御部42を起動する（ステップS13）。この制御部42は、すべての命令をサーバサイドで処理し、前記端末機器に適切なコマンドを与えてこれを制御する。

また、前記リストから端末名を選択することで、選択に係るIPv6端末にルーティングされて接続されるようになっていても良い。また、検索条件  
15 で特定の状態を入力して検索し、その端末が見つかった場合には、直接当該端末に接続するようにしても良い。なお、InterServer6を介したトンネリング接続によらずに外部からWebサーバを通して当該端末の検索を行った場合でも、当該端末への接続はトンネリング接続を確立してから行なわれるようになっている。

20 ここで、上記「トンネリング」とは、IPv6ネットワーク（ルータ）同士をIPv4ネットワークを介して接続するための技術であり、特定ルータ間でIPv6パケットをIPv4でカプセルングしてやり取りするための技術である。

なお、上記InterBOX3及びInterServer6の前記各構成要素10～42は、実際にはコンピュータシステムに設けられたハードディスクに確保された一定の領域及びそこにインストールされたコンピュータソフトウェアプログラム、これらのハードディスクを制御して前記プログラムを読み出して実行するためのCPU、RAM、その他入出力装置等の周辺  
25

機器から構成される。

- また、前記InterBOX3は、各端末2を含む1つのコンピュータシステムから構成されていることが好ましいが、前記InterServer6は、負荷を分散するために互いに接続された複数のコンピュータシステムから構成されていることが好ましい。例えば、InterBOX3やIPv6端末2やホームネットワークの状態を管理をする端末検索部26は、専用の送受信インタフェース及び制御部を有するサーバによって構成されていることが好ましい。各機器のON/OFFやその他の状態を管理するというセッションは膨大になることが予想され、負荷分散が必要であるからである。
- 10 また、1つのInterServer6で複数の異なるメーカーのInterBOXやIPv6端末に対応する場合、前記カプセリング処理部18や、コマンド設定部22、フィルタ部23等は複数設けられていても良い。

次に、上記InterBOX3及びInterServer6の動作を、図10以下の通信例を参照して詳しく説明する。

- 15 図10は、InterBOX3が接続されているホームネットワークのIPv6端末2と、前記InterServer6に直接若しくはIPv6ホームネットワーク1aを介して接続されているIPv6サーバ7との間で通信を行う場合を示したものである。

- この例では、前記InterServer6には、この図に示すように、
- 20 前記IPv6端末2のIPv6アドレス16aとInterBOXのIPv4グローバルアドレス16bが予め記憶されていることが前提となっている。このため、前記IPv6端末2は、予め例えば前記InterBOX3若しくは他の手段を通して前記InterServer6に対して自己のIPv6アドレスを知らせておく必要がある。この動作は、たとえば、ユーザが
- 25 自己のIPv6端末2を前記ホームネットワーク1に接続することで、プラグアンドプレイ機能により、自動的に前記InterBOX3に前記InterServer6との間にトンネリング接続が確立され、達成されるようになっていても良い。前記InterServer6は、このIPv6端末

2のIPv6アドレス若しくはその一部（InterServerのIPv6アドレスプレフィックス）が分かると、当該IPv6アドレスへのルーティングがこのInterServer6を通して行なわれるように他のISPルータにアナウンス（広報）するようになっている。

- 5     なお、前記IPv6端末2のIPv6アドレスが前記InterBOX3に割当てられたプレフィックスに依存する場合には、前記InterServer6に記憶されるIPv6端末2のアドレス16aとして、このアドレス16aの一部を構成する前記InterBOX3のIPv6プレフィックスを格納しておくだけでも良い。そして、この場合には、前記InterServer6は、そのプレフィックスのルーティング情報を他のISPルータにアナウンスするようにする。

10     以上のような処理及び設定（トンネリング接続）がすでになされている状態で、前記IPv6サーバ7側から前記IPv6端末2への接続リクエストがなされると、このIPv6サーバ7からの接続はInterServer6にルーティングされる。InterServer6は前記IPv6端末2のアドレス16aから前記InterBOX3のIPv4アドレスを割り出し、前記トンネリングセッション確立部17、11により前記InterBOX3との間でトンネリング接続内の通信セッションを確立させる。

20     そして、トンネリング通信セッションが確立されると、前記IPv6端末2へのパケットは、前記カプセリング処理部18によって前記InterBOX3向けのIPv4パケットでカプセリングされて送信される。InterBOX3は、カプセリング処理部12がそのパケットをディカプセリングすると共に、前記ルーティング処理部13が前記パケットに含まれているIPv6端末2のアドレスに基づいて前記IPv6端末2へのルーティング処理を行う。このようにして、例えば家庭内のIPv6ホームネットワーク上のIPv6端末2への接続を、外部にあるIPv6サーバ7側からの起動により行うことができる。

例えば、前記IPv6端末2が家庭内監視カメラであるとする、外出中

であっても、自己のPDA等を身近にあるIPv6ネットワークに接続することによって前記InterServer6及びInterBOX3を介して前記カメラを起動・制御することが可能になる。

また、この例では、端末2の機種に応じてInterServer6に設  
5 けられたIPv6端末機種判別部21、コマンド設定部22及びフィルタ部23が機能するようになっている。

前記機種判別部21は、例えば前記IPv6端末のIPv6アドレス（アドレスそれ自体若しくはアドレスに関連付けられた情報）に基づいて当該IPv6端末2の機種やネットワーク環境を判別するように構成されている。  
10 この実施形態では、前記IPv6端末2およびInterServer6は同じメーカー、若しくは統一された規格に基づいて製造されることが想定されており、この場合、各端末2にあらかじめ割当てられる（若しくは生成される）IPv6アドレスに一定のルールを設定しておくことで、このアドレスを知るだけで容易にこの機種の種別及びネットワークの環境を判別することが  
15 できる。この実施形態では、前記IPv6アドレス中の前記プレフィックス部とMACアドレス部とに基いて、メーカー及び機種を判別する。

また、このIPv6端末2の制御に特別なコマンドが必要な場合、前記機種別コマンド設定部22が前記IPv6サーバ7からの通信に含まれる命令をこの機種用のコマンドに変換して設定する。例えば、Html言語で記述  
20 されたメッセージから所定のコマンドを生成するようにしても良い。また、1つのサーバ7からの命令を複数のIPv6端末2のためのコマンドに変換するようにしても良い。

さらに、前記フィルタ部23は、所定のルールに基づいてこのInterServer6を通過するIPv6パケットをフィルタリングする機能を有  
25 するものである。このフィルタリングのルールは、例えば、接続先のIPv6端末2毎に設定されていても良いし、ネットワーク毎に設定されていても良い。なお、前記機種判別部21で所定の機種やネットワーク環境でないと判断された場合や、前記フィルタ部23で適切でないと判断された場合には

前記通信セッション切断部が通信セッションを切断するように構成されている。また、接続先のIPv6端末の電源がOFF等で接続できない場合においても、同じInterBoxに接続された他のIPv6機器で代替可能なものであれば前記機種や種別情報に基づいて当該他のIPv6端末にルーティングするようにしても良い。

また、図11は、共にInterBOX3、3'を有するIPv6ホームネットワーク同士がInterServer6を介して接続する場合の例である。各ホームネットワークには、IPv6端末AとIPv6端末Bがそれぞれ接続されており、この2つのIPv6端末A、B間で通信を行う場合を例にとって説明する。

この場合にも、前記InterServer6には、IPv6端末A、Bのそれぞれのアドレス若しくはその一部（IPv6プレフィックス）が、それぞれのInterBOX3のIPv4アドレスに関連付けて格納されている。

そして、一方の端末Aから他方の端末Bへの接続が要求されると、まず、端末A側のInterBOX・AとInterServer6との間にトンネル接続内での通信セッションが確立される。そして、そのパケットに含まれる端末Bのアドレスに基づいて前記InterBOX・Bが特定され、これにより、このInterServer6とInterBOX・Bとの間でのトンネリング通信セッションが確立される。そして、このInterBOX・Bでは、パケットに含まれる端末BのIPv6アドレスに基づいてネットワーク内でのルーティングを行う。

これにより、2つのIPv6端末同士が、前記InterServer6を介してIPv6により通信を行うことが可能になる。

なお、このように2つのIPv6端末間で通信を行いたい場合において、接続先のIPv6端末のアドレスが不明な場合がある。この場合には、接続元のユーザは、前記InterServer6にアクセスし、前記IPv6端末検索部26を起動する。このとき、セキュリティのため、前記接続要

求認証部 27 がこのユーザの認証を行い、正当な接続要求であるかを判断した後、接続先の IPv6 端末やユーザの検索を許可する。そして、所望の IPv6 端末が特定できた場合には、この端末の IPv6 アドレスに基づいてトンネル通信セッションが確立されるようになっている。

- 5     以上のような構成によれば、IPv6 端末 2 に関する全ての通信はキャリアや ISP に関らず、前記 InterServer 6 を通して行われることになるから、家庭や職場のホームネットワーク上の IPv6 端末 2 やサーバ 7 を前記 InterServer 6 の所有者が自由に設定・制御することが可能になる。これにより、従来問題であった、IPv6 と IPv4 が混在する中での IPv6 機器の個体認識、家庭内ルーティング及びセキュリティの問題を全て解決でき、極めてオープンかつ、クローズドなネットワークの構築を実現することが可能になる。
- 10

- また、この InterServer 6 の所有者は、通常 IPv6 端末 2 の製造者であるメーカーであることが想定される。したがって、このメーカー
- 15    はこの InterServer 6 に対応する自社の IPv6 機器のラインアップを用意することで、インターネットを利用した付加価値を生み出すことが可能になる。

次に、図 12 に基づいて前記 IPv6 端末 2 のサインアップについて説明する。

- 20    すなわち、上記の説明においては、IPv6 端末 2 の IPv6 アドレスは前記 InterBOX 3 側から受け取るものとしたが、実際には、この方法以外にも様々な方法が考えられる。また、メーカーや InterServer 6 の所有者としては、IPv6 端末 2 の所有者（ユーザ）の情報を知りたいと考えられる。さらに、IPv6 端末 2 のアドレスの生成方法についても
- 25    、前述したように予め工場出荷の段階で各端末に固定 IPv6 アドレスが RAM 等へ書き込まれている場合もあるであろうし、接続する InterBOX 3 の IPv6 プレフィックスに依存して決められる場合もあると考えられる。



したがって、この実施例では、例えば、図12に示すように、IPv6端末2若しくはInterBOX3のユーザは、まずユーザ管理サーバ30に接続して、ユーザ登録を行うようになっている。このユーザ登録はIPv6  
5 端末2を用いてInterBOX3を通して行うようにしても良いし、既存のパソコン等のIPv4通信対応機器を利用して行うようにしても良い。ここでは、IPv6端末2及びInterBOX3を通して行う場合について説明する。また、以下では、IPv6端末2のIPv6アドレスが、InterBOX3に割り付けられるIPv6アドレスプレフィックスと各端末2のMACアドレスとを組み合わせる場合を例にとって説明する。

10 この場合、まず、ユーザが前記IPv6端末をInterBOX3に接続すると、このInterBOX3がISP/キャリアを介してユーザ管理サーバ30に接続する。このことで、InterBOX3から前記IPv6プレフィックスの他前記InterServer6との間のトンネリング接続に必要な情報等がこのユーザ管理サーバ30に通知される。また、ユーザは  
15 、そのユーザ、InterBOX3若しくはIPv6端末2を特定するための情報や端末2の種別に関する情報、ネットワーク1に関する情報、その他課金に必要な情報等をこのInterBOX3を通して前記管理サーバ30に通知する。この例では、当該InterBOX3若しくは各ユーザ毎にIDおよびパスワードが発行され、前記InterBOX3およびユーザの情報  
20 報はこれに関連付けデータベース31に登録される。なお、登録に必要な情報はこれに限るものではなく、他の情報が必要になることも考えられるし、逆に、パスワードや課金情報等が不要な場合にはこれらの情報を登録する必要はない。

25 なお、前記InterBOX3のIPv6アドレスプレフィックスは、予めこのInterBOX3に製造時等に割り振られて格納されているものであっても良いし、このようにユーザ登録することによって初めてサーバ側から通知されるものであっても良い。また、後者の場合において、ユーザ登録をInterBOX3を通さずに既存のパソコン等を用いてインターネット

上で行う場合には、前記IPv6プレフィックスや前記ID及びパスワードを手動でこのInterBOX3に設定するようにする。そして、このようなユーザ登録が終了すると、前記InterBOX3やIPv6端末2にも接続に必要な情報が格納される。この場合、前記InterServerに

5 設けられた機種判別部は、ユーザに登録された情報に基づいて機種判別を行うようにしても良い。

上記のようなユーザ管理サーバ30は、前記InterServer6に接続されているものであっても良いし、インターネット上にそれとは独立的に設けられていても良い。

10 一方、図13は、トンネリング接続及びその中での通信セッションの確立の具体的方法に関する実施例を示すものである。この図中に示されたS2.1～S27の各符号は、以下の各ステップS21～S27に対応するものである。

まず、上記で説明した実施例においては、InterBOX3はInterServer6のIPv4アドレスを記憶していたが、これは、メーカー

15 が工場出荷時に予めRAMに記録する方法であっても良いし、実際のトンネリング接続時に他のサーバ等から受け取って設定する方法であっても良い。InterServer6が単一の場合には前者でも良いが、InterServer6が複数ある場合には後者による方法の方が効率的であると考え

20 られる。

この図の例は後者の場合であり、そのためにトンネルブローカー52が設けられている。このトンネルブローカー52は、前記ユーザ情報管理DB31を参照することができるように構成されている。また、このトンネルブローカー52には、InterServer6及びInterBOX3のIPv4アドレスを格納するアドレスデータベース53が接続されている。そして、前記InterBOX3には予めこのトンネルブローカー52のIPv4グローバルアドレスが設定されている。また、InterBOX3には、

25 上記で設定したIDおよびパスワード（必要な場合）が既に設定されている

ものとする。

この場合、前記InterBOX3は、まず、トンネルブローカー52に接続し、前記IDおよびパスワードを送信する(ステップS21)。このことで、このトンネルブローカー52は、前記InterBOX3の認証を行うと共に、このInterBOX3のIPv6アドレスプレフィックスを得る(ステップS22)。ついで、このトンネルブローカー52は、前記アドレスデータベース53からトンネル接続を確立する先のInterServer6を選択し(ステップS23)、前記InterBOX3にこのInterServer6のIPv4アドレスを通知する(ステップS24)。また、トンネルブローカー52は、InterBOX3のIPv4アドレスと、IPv6端末識別用のIPv6プレフィックス(IPv6端末2のアドレスの一部)をInterServer6側に渡す(ステップS25)。このことで、前記InterBOX3はInterServer6を識別可能になり、トンネリングセッションを確立することができる(ステップS26, S27)。また、InterServer6は、通知されたIPv6プレフィックスのルーティングを他のルータにアナウンスする。ことにより、当該プレフィックスを持つIPv6アドレスのルーティングは全てこのInterServer6にルーティングされることになる。

このような構成によれば、InterServer6が複数存在する場合であっても、そのうちの1つとの間で確実にトンネリング接続を確立することができる。なお、上記では、前記トンネリングブローカー52でユーザや端末の認証を行ったが、これに限定されるものではない。前記トンネリングブローカー52は、前記InterBox2に前記InterServer6のアドレスのみを知らせ、前記InterServer6がユーザ認証を行うようにしても良い。また、このとき、InterServer6がInterBox2や端末3に対して任意のアドレスを付与するようにしても良い。

なお、以上説明した実施形態は、この発明の一つの実施形態に過ぎないの

であって、その要旨を変更しない範囲で種々の形態をとりうることはいうまでもない。

例えば、上記一実施形態では、InterBOX3側からもInterServer6側からも、トンネリング接続を確立できるようにしているが、  
5 実際の商用サービスではInterBOX3からの起動のみであることが一般的であると考えられる。IPv4の固定IPサービス自体がまれであるからである。すなわち、この場合、一度トンネリング（実際にはIPv4接続それ自体）が確立した後は、設定はそのまま残り、一度IPv4のセッションが切れてしまえば、次にInterBox3のIPv4が同一であること  
10 の方が珍しいため、実際にIPv4のセッション自体が切断されているとルーティングも出来ないからである。

また、上記一実施形態では、前記第1のプロトコルはIPv6、第2のプロトコルとしてIPv4を例に取って説明したがこれに限定されるものではない。第2のプロトコルもIPv6であってもよい。また、第1、第2の  
15 プロトコル共にIPv4であってもよい。さらに、両方ともに上記以外のプロトコルであっても良い。

前記一実施形態では、前記InterBox3は、各端末とは独立して設けられていたが、InterBOX3自体がIPv6端末であってもよいし、InterBOX3がいずれかの端末2若しくは各端末2にハードウェア的  
20 若しくはソフトウェア的に一体化されて構成されていても良い。この場合、上記InterBOX3は、1つのホームネットワークに複数設けられていても良い。

## 請求の範囲

1. クライアント機器が接続され第1の通信プロトコルで通信が行われる第1のネットワークに設けられた中継装置と、この中継装置が第2のネットワークを通し第2の通信プロトコルで接続されるサーバとを有し、
- 5 前記中継装置には、前記クライアント機器の前記第1の通信プロトコルでのグローバルアドレスを記憶する前記クライアント機器グローバルアドレス記憶部と、前記サーバの第2のプロトコルでのグローバルアドレスを記憶するサーバアドレス記憶部と、この記憶部に記憶されたサーバのグローバルアドレスに基づき前記クライアント機器からの接続を前記サーバを経由するよう
- 10 うにルーティングするための第1のルーティング装置と、第1のプロトコルでのパケットを第2のプロトコルでカプセリング／デカプセリングすることで前記サーバとの間で第1のプロトコルのトンネリング接続を確立する第1のパケット処理装置と、が設けられており、  
前記サーバには、前記中継装置との間のトンネリング接続を可能にするため
- 15 に第1のプロトコルでのパケットを第2のプロトコルでカプセリング／デカプセリングする第2のパケット処理装置と、前記中継装置に接続された前記クライアント機器の第1のプロトコルでのグローバルアドレスを前記中継装置の第2のプロトコルでのグローバルアドレスに関連付けて管理する端末機器グローバルアドレス管理装置と、この管理装置で管理された前記端
- 20 末機器のグローバルアドレスに基づいて前記中継装置へのルーティングを行う第2のルーティング装置と、が設けられている  
ことを特徴とするインターネット接続システム。
2. 請求項1記載のインターネット接続システムにおいて、  
前記第1のプロトコルと第2のプロトコルは、異なるプロトコルであるこ
- 25 とを特徴とするシステム。
3. 請求項1記載のインターネット接続システムにおいて、  
前記第1のプロトコルと第2のプロトコルは、同じプロトコルであることを特徴とするシステム。

4. 請求項 1 記載のインターネット接続システムにおいて、  
前記サーバには、前記クライアント機器若しくは／及び前記中継装置が所定の機種であるかを判別する機種判別部が設けられていることを特徴とするシステム。
5. 請求項 4 記載のシステムにおいて、  
前記サーバには、前記機種判別部により前記クライアント機器若しくは中継装置が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部が設けられていることを特徴とするシステム。
10. 6. 請求項 4 記載のインターネット接続システムにおいて、  
前記サーバには、前記機種判別部による判断結果に基づいて前記クライアント機器に送信する命令をこのクライアント機器を制御するための所定形式のコマンドに変換するコマンド変換部が設けられていることを特徴とするシステム。
15. 7. 請求項 4 記載のインターネット接続システムにおいて、  
前記サーバには、前記機種判別部による判断結果に基づいて前記クライアント機器を制御するクライアント機器制御部が設けられていることを特徴とするシステム。
8. 請求項 1 記載のインターネット接続システムにおいて、  
前記サーバには、前記クライアント機器若しくは／及び中継装置が接続された第 1 のネットワークの環境が所定の種別であるかを判別するネットワーク種別判別部が設けられていることを特徴とするシステム。
20. 9. 請求項 8 記載のシステムにおいて、  
前記サーバは、前記クライアント機器若しくは中継装置が接続されたプライベートネットワーク環境が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部を有することを特徴とするシステム。
25. 10. 請求項 9 記載のシステムにおいて、

前記サーバは、前記クライアント機器若しくは／及び中継装置の動作状態、使用状態、位置情報の少なくとも1つ又は複数の情報を取得する状態情報取得部を有することを特徴とするシステム。

1 1. 請求項 1 0 記載のシステムにおいて、

- 5 前記状態情報取得部は、前記クライアント機器の機種に応じた方法で前記クライアント機器の動作状態、使用状態、位置情報の少なくとも1つ又は複数の情報を取得するものであることを特徴とするシステム。

1 2. 請求項 1 0 記載のシステムにおいて、

- 10 前記サーバは、前記クライアント機器若しくは中継装置のアドレス、動作状態、使用状態、位置情報の少なくとも1つ又は複数の情報を組み合わせた情報に基づいて前記クライアント機器若しくは中継装置を検索する検索部を有することを特徴とするシステム。

1 3. 請求項 1 1 記載のシステムにおいて、

- 15 前記検索部は、前記中継装置毎にこの中継装置に接続されたクライアント機器を一覧表示する手段を有することを特徴とするシステム。

1 4. 請求項 1 3 記載のインターネット接続システムにおいて、

前記サーバには、前記クライアント機器を制御するクライアント機器制御部が設けられており、

- 20 このクライアント機器制御部は、前記一覧表示から特定のクライアント機器を選択することでこのクライアント機器に対応するクライアント制御プログラムを起動させるものであることを特徴とするシステム。

1 5. 請求項 1 記載のシステムにおいて、

- 25 前記サーバには、前記クライアント機器への接続要求に基づいて前記クライアント機器の第1のプロトコルでのグローバルアドレスの検索を行うクライアント機器アドレス検索部が設けられていることを特徴とするシステム。

1 6. 請求項 1 5 記載のシステムにおいて、

前記サーバには、前記クライアント機器への接続要求を行った者の認証を行って前記クライアント機器への接続を許可若しくは否認する接続要求者認

証部が設けられていることを特徴とするシステム。

17. 請求項1記載のシステムにおいて、

このシステムはさらに、前記中継装置とサーバとの間のトンネリング接続情報を管理するトンネリング接続情報管理装置を有し、

5 このトンネリング接続情報管理装置は、前記サーバの第2の Protokolでのグローバルアドレスを前記中継装置に通知し、前記中継装置の第2の Protokolでのグローバルアドレス及び前記クライアント機器の第1の Protokolでのグローバルアドレス若しくはその一部を前記サーバに通知することを特徴とするシステム。

10 18. 請求項17記載のシステムにおいて、

前記トンネリング接続情報管理装置は、前記中継装置若しくはサーバの認証を行い、その結果が肯定的である場合に前記通知を行うことを特徴とすることを特徴とするシステム。

19. 請求項1記載のインターネット接続システムにおいて、

15 前記サーバは、前記クライアント機器への／からの通信を所定のルールでフィルタリングするフィルタリング処理装置を有することを特徴とするシステム。

20. 請求項19記載のシステムにおいて、

前記サーバは、前記所定のルールを編集するためのインタフェースを提供  
20 するフィルタリングルール設定部をさらに有することを特徴とするシステム。

21. 請求項1記載のインターネット接続システムにおいて、

前記中継装置には、前記クライアント機器が所定の機種であることを判別する機種判別部が設けられていることを特徴とするシステム。

25 22. 請求項20記載のインターネット接続システムにおいて、

前記中継装置には、前記機種判別部により前記クライアント機器が所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断する通信セッション切断部が設けられていることを特徴とするシステム。



23. クライアント機器が接続され第1の通信プロトコルで通信が行われる第1のネットワークに設けられた中継装置と、この中継装置が第2のネットワークを通し第2の通信プロトコルで接続されるサーバと、を有するインターネット接続システムに使用される前記中継装置であって、

- 5 前記中継装置には、前記クライアント機器の前記第1の通信プロトコルでのグローバルアドレスを記憶する前記クライアント機器グローバルアドレス記憶部と、前記サーバの第2のプロトコルでのグローバルアドレスを記憶するサーバアドレス記憶部と、この記憶部に記憶されたサーバのグローバルアドレスに基づき前記クライアント機器からの接続を前記サーバを経由するよう
- 10 うにルーティングするための第1のルーティング装置と、第1のプロトコルでのパケットを第2のプロトコルでカプセリング／デカプセリングすることとで前記サーバとの間で第1のプロトコルのトンネリング接続を確立する第1のパケット処理装置と、が設けられていることを特徴とする中継装置。

24. クライアント機器が接続され第1の通信プロトコルで通信が行われる第1のネットワークに設けられた中継装置と、この中継装置が第2のネットワークを通し第2の通信プロトコルで接続されるサーバと、を有するインターネット接続システムに使用される前記サーバであって、
- 15

- 前記サーバには、前記中継装置との間のトンネリング接続を可能にするために第1のプロトコルでのパケットを第2のプロトコルでカプセリング／デ
- 20 イカプセリングする第2のパケット処理装置と、前記中継装置に接続された前記クライアント機器の第1のプロトコルでのグローバルアドレスを前記中継装置の第2のプロトコルでのグローバルアドレスに関連付けて管理する端末機器グローバルアドレス管理装置と、この管理装置で管理された前記端末機器のグローバルアドレスに基づいて前記中継装置へのルーティングを行う
- 25 第2のルーティング装置と、が設けられていることを特徴とするサーバ。

25. 第1のネットワークに設けられた中継装置と、この第1のネットワークに接続されたクライアント機器が前記中継装置及びインターネットを通して接続されるサーバと、を有するインターネット接続システムに使用される

前記サーバであって、

前記中継装置に接続された前記クライアント機器のアドレスを前記中継装置のアドレスに関連付けて管理するクライアント機器アドレス管理装置と、

前記インターネットから前記クライアント機器宛の接続を、前記管理装置  
5 で管理された前記クライアント機器のアドレスに基づいて前記クライアント機器が接続された中継装置へルーティングするルーティング装置と、

前記クライアント機器若しくは／及び前記中継装置が所定の機種であるかを判別する機種判別部と、

前記機種判別部による判断結果に基づいて前記クライアント機器に送信する命令をこのクライアント機器を制御するための所定形式のコマンドに変換するコマンド変換部と  
10

を有することを特徴とするサーバ。

26. 請求項25記載のサーバにおいて、

さらに、前記機種判別部により前記クライアント機器若しくは中継装置が  
15 所定の種別でないと判断された場合、それに基づいて当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部が設けられていることを特徴とするサーバ。

27. 請求項25記載のサーバにおいて、

前記クライアント機器は、前記中継装置とは通信可能であるが、自らはインターネットに接続することができない周辺装置を含むものであることを特徴とするサーバ。  
20

28. 請求項25記載のサーバにおいて、

さらに、前記クライアント機器若しくは／及び中継装置が接続された第1のネットワークの環境が所定の種別であるかを判別するネットワーク種別判別部が設けられていることを特徴とするサーバ。  
25

29. 請求項28記載のサーバにおいて、

さらに、前記クライアント機器若しくは中継装置が接続されたプライベートネットワーク環境が所定の種別でないと判断された場合、それに基づいて

当該通信セッションを切断若しくはパケットの送受信を制限する通信セッション切断部を有することを特徴とするサーバ。

30. 請求項25記載のサーバにおいて、

さらに、前記クライアント機器若しくは／及び中継装置の動作状態、使用  
5 状態、位置情報の少なくとも1つ又は複数の情報を取得する状態情報取得部を有することを特徴とするサーバ。

31. 請求項30記載のサーバにおいて、

前記状態情報取得部は、前記クライアント機器の機種に応じた方法で前記  
クライアント機器の動作状態、使用状態、位置情報の少なくとも1つ又は複数  
10 の情報を取得するものであることを特徴とするサーバ。

32. 請求項30記載のサーバにおいて、

さらに、前記クライアント機器を制御するクライアント機器制御部が設け  
られており、

このクライアント機器制御部は、前記クライアントの動作状態、使用状態  
15 、位置情報の少なくとも1つの情報をユーザに表示する手段を有するものである

ことを特徴とするサーバ。

33. 請求項30記載のサーバにおいて、

さらに、前記クライアント機器若しくは中継装置のアドレス、動作状態、  
20 使用状態、位置情報の少なくとも1つ又は複数の情報を組み合わせた情報に基づいて前記クライアント機器若しくは中継装置を検索する検索部を有することを特徴とするサーバ。

34. 請求項33に記載のサーバにおいて、

前記検索部は、検索されたクライアント機器をその動作状態と共に一覧表  
25 示する一覧表示手段を有することを特徴とするサーバ。

35. 請求項34に記載のサーバにおいて、

前記一覧表示手段は、前記中継装置毎にこの中継装置に接続されたクライアント機器を一覧表示するものであることを特徴とするサーバ。

36. 請求項34記載のサーバにおいて、

さらに、前記クライアント機器を制御するクライアント機器制御部が設けられており、

このクライアント機器制御部は、前記一覧表示から特定のクライアント機器を選択することでこのクライアント機器に対応するクライアント制御プログラムを起動させるものであることを特徴とするサーバ。

37. 請求項25記載のサーバにおいて、

前記中継装置は、前記クライアント機器に設けられているものであることを特徴とするサーバ。

10 38. 請求項25記載のサーバにおいて、

さらに、前記中継装置との間のトンネリング接続を可能にするために第1の protokolでのパケットを第2の protokolでカプセルリング/デカプセルリングする第2のパケット処理装置と、前記中継装置に接続された前記クライアント機器の第1の protokolでのグローバルアドレスを前記中継装置の第2の protokolでのグローバルアドレスに関連付けて管理する端末機器グローバルアドレス管理装置と、この管理装置で管理された前記端末機器のグローバルアドレスに基づいて前記中継装置へのルーティングを行う第2のルーティング装置とが設けられていることを特徴とするサーバ。

20 39. 請求項38記載のサーバにおいて、

前記第1の protokolと第2の protokolは、異なる protokolであることを特徴とするサーバ。

40. 請求項38記載のインターネット接続システムにおいて、

前記第1の protokolと第2の protokolは、同じ protokolであることを特徴とするシステム。

41. 請求項38記載のサーバにおいて、

さらに、前記クライアント機器への接続要求に基づいて前記クライアント機器の第1の protokolでのグローバルアドレスの検索を行うクライアント

機器アドレス検索部が設けられていることを特徴とするサーバ。

4 2. 請求項 4 1 記載のサーバにおいて、

さらに、前記クライアント機器への接続要求を行った者の認証を行って前記クライアント機器への接続を許可若しくは否認する接続要求者認証部が設

5 けられていることを特徴とするサーバ。

4 3. 請求項 3 8 記載のサーバにおいて、

さらに、前記中継装置とサーバとの間のトンネリング接続情報を管理するトンネリング接続情報管理装置を有し、

このトンネリング接続情報管理装置は、前記サーバの第 2 のプロトコルで  
10 のグローバルアドレスを前記中継装置に通知し、前記中継装置の第 2 のプロトコルでのグローバルアドレス及び前記クライアント機器の第 1 のプロトコルでのグローバルアドレス若しくはその一部を取得するものである

ことを特徴とするサーバ。

4 4. 請求項 4 3 記載のサーバにおいて、

15 前記トンネリング接続情報管理装置は、前記中継装置の認証を行い、その結果が肯定的である場合に前記通知を行うことを特徴とすることを特徴とするサーバ。

4 5. 請求項 3 8 記載のサーバにおいて、

さらに、前記クライアント機器への／からの通信を所定のルールでフィル  
20 タリングするフィルタリング処理装置を有することを特徴とするサーバ。

4 6. 請求項 4 5 記載のサーバにおいて、

さらに、前記所定のルールを編集するためのインタフェースを提供するフィルタリングルール設定部を有することを特徴とするサーバ。

図 1

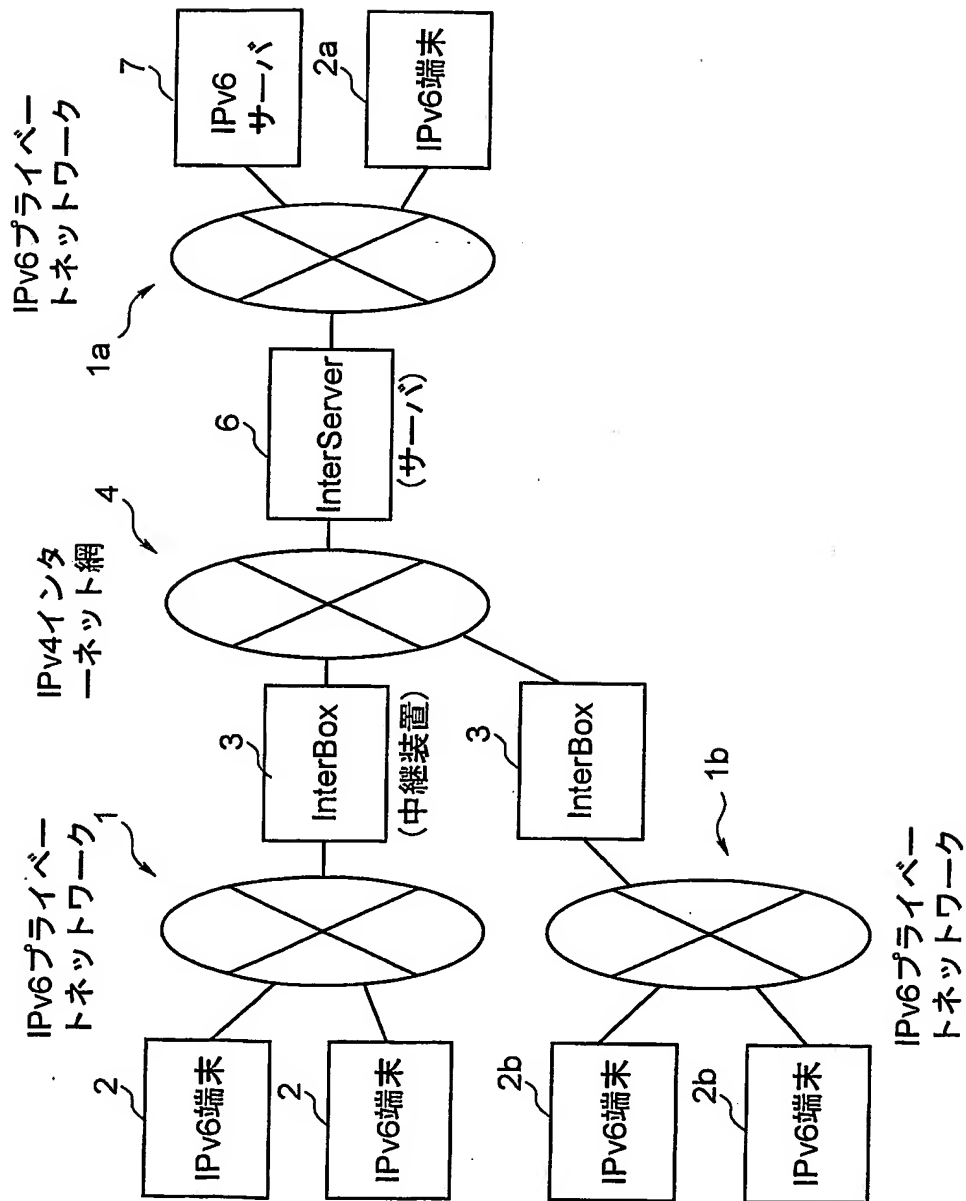


図 2

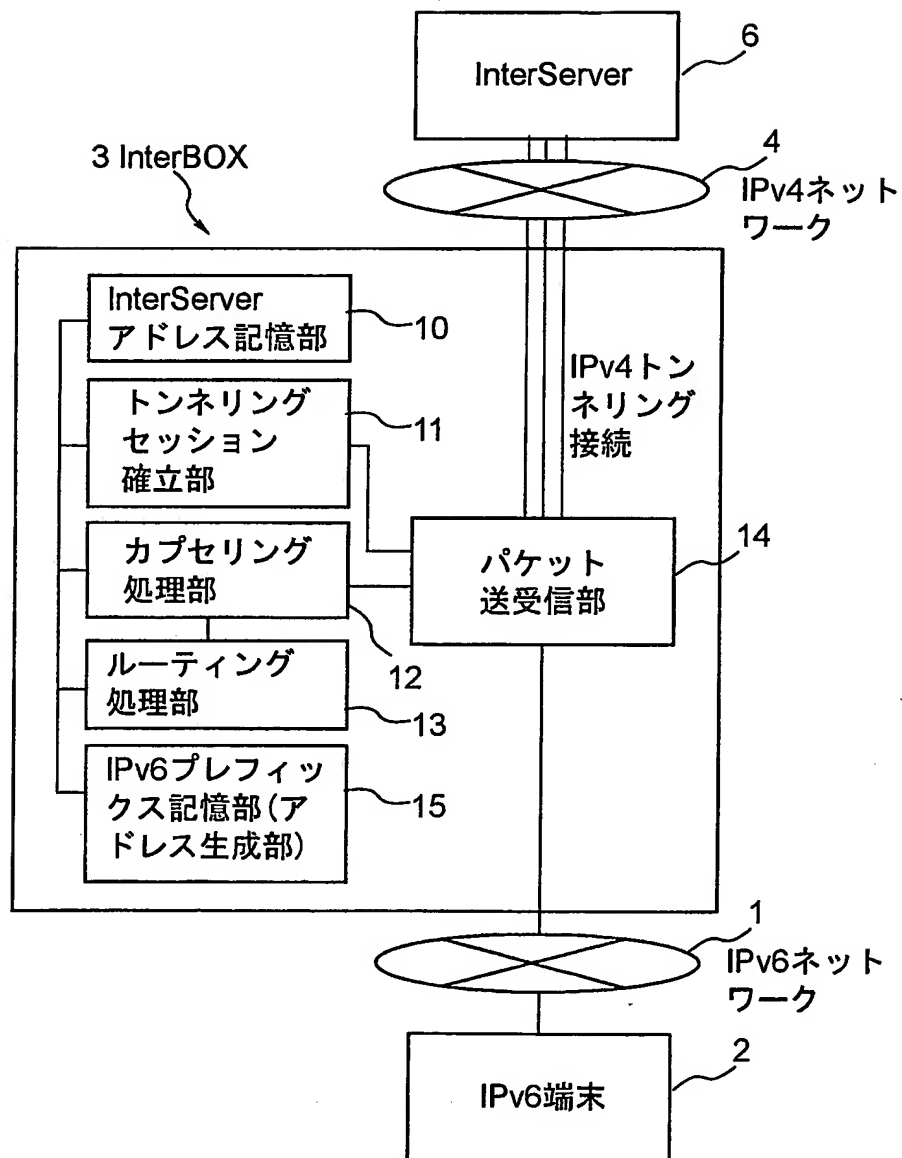


図 3

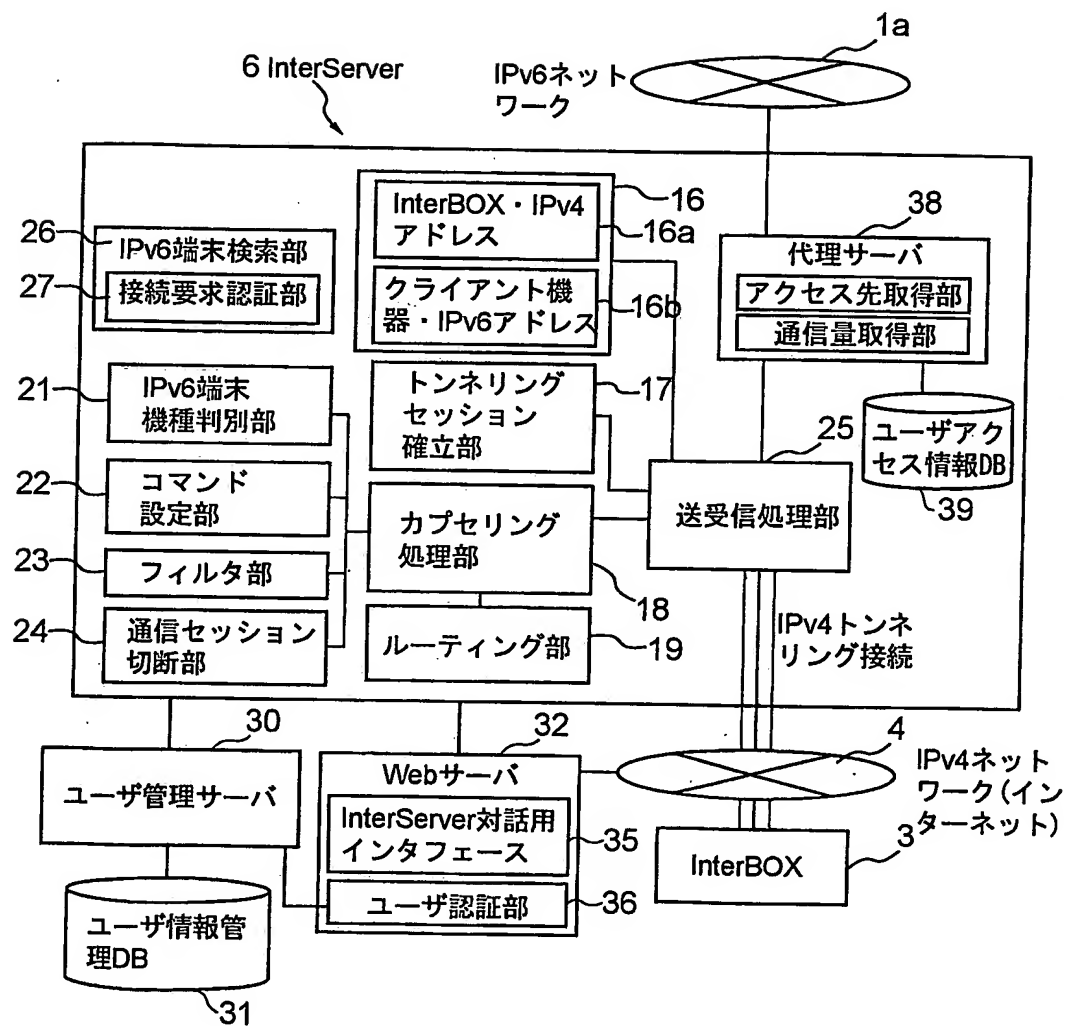




図 4

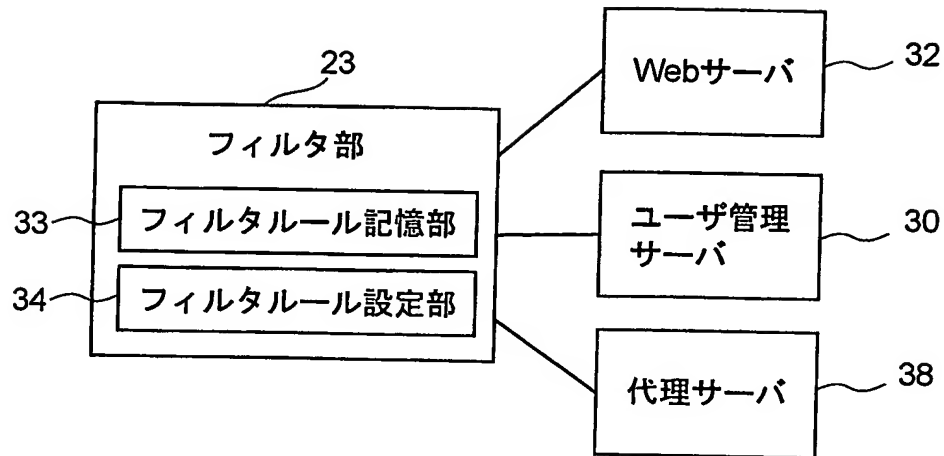


図 6

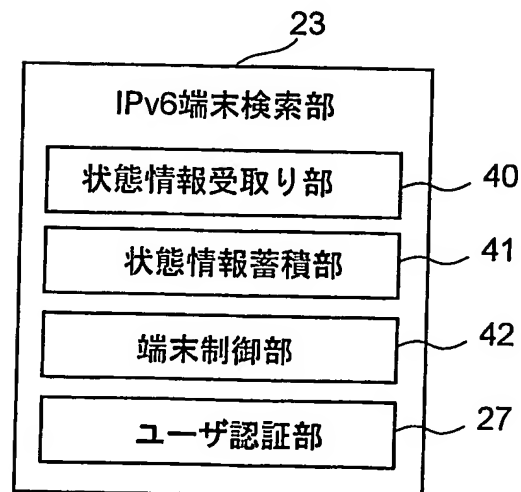


図 5

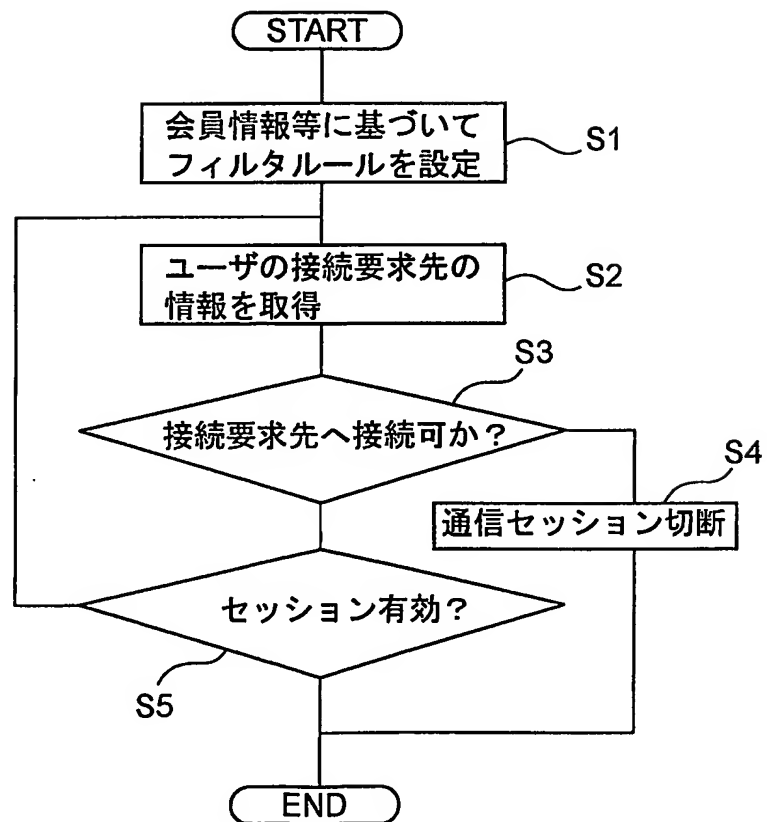


図 8

InterBOX名 (アドレス/プレフィックス):

IPv6端末名	所有者	状態	種別	機種名		
1	父	電源ON	ビデオ	XX1	操作画面	45
2	父	電源ON	テレビ	YY2	操作画面	45
3	父	電源OFF	PC	SS3	操作画面	45
4	父	電源ON	カメラ	FF4	操作画面	45

図 7

検索用インターフェース

InterBOX情報

InterBOX名 (ドメイン名/プレフィックス):

ロケーション:

IPv6端末情報

状態情報

機種情報

種別情報

検索開始 キャンセル

図 9

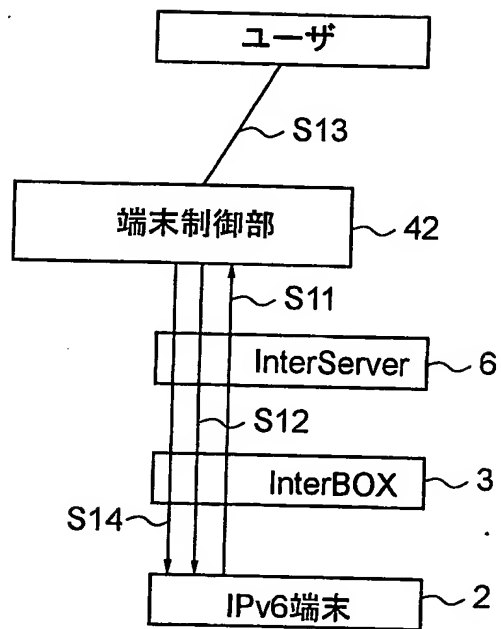


図 1 0

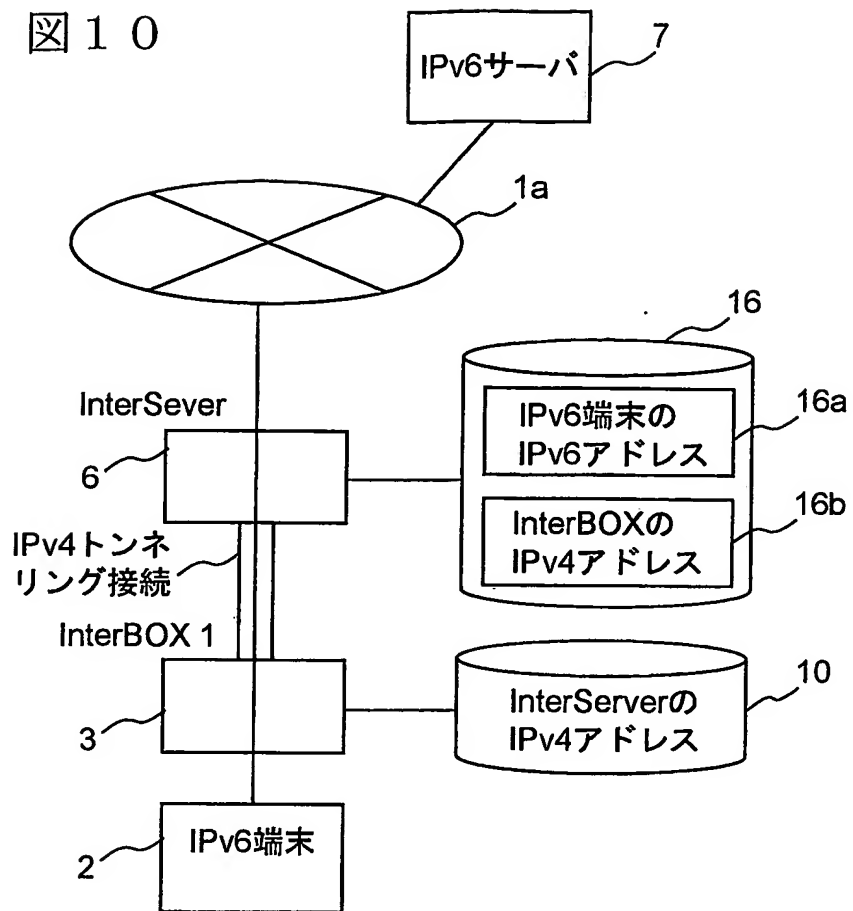


図 1 1

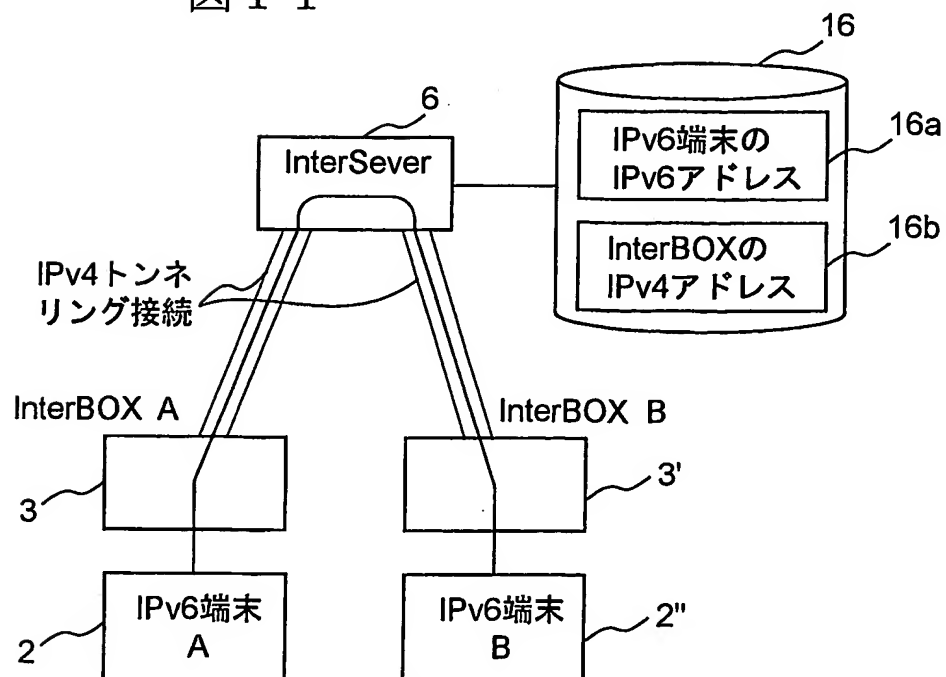


図 1 2

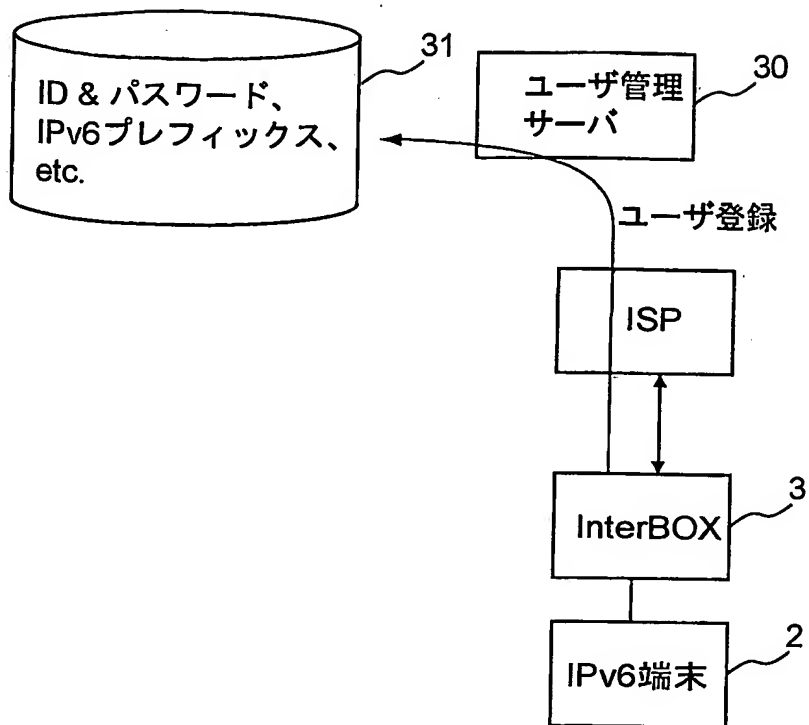


図 1 3

